ELSEVIER

Theoretical Computer Science (2002) 235–249

Theoretical Computer Science

www.elsevier.com/locate/tcs

Reconstructing permutation matrices from diagonal sums ☆

Alberto Del Lungo

Dipartimento di Matematica, Universita di Siena, Via del Capitano 15, 53100 Siena, Italy

Abstract

In this paper, we present a result concerning the reconstruction of permutation matrices from their diagonal sums. The problem of reconstructing a sum of k permutation matrices from its diagonal sums is $\mathbb{NP}$-complete. We prove that a simple variant of this problem in which the permutation matrices lie on a cylinder instead of on a plane can be solved in polynomial time. We give an exact, algebraic characterization of the diagonal sums that correspond to a sum of permutation matrices. Then, we derive an $O(kn^2)$-time algorithm for reconstructing the sum of k permutation matrices of order n from their diagonal sums. We obtain these results by means of a generalization of a classical theorem of Hall on the finite abelian groups.

Keywords: Combinatorial problem; Discrete tomography; Permutation; Permutation matrix; Diagonal sum; Finite abelian group

1. Introduction

A *lattice set* is a finite subset of the integer lattice $\mathbb{Z}^2$. It can be represented by a $(0,1)$-matrix [1] as shown in Fig. 1. A *discrete* X-ray of a lattice set in a direction u is the function giving the number of points on each line parallel to u (see Fig. 1). Discrete Tomography studies the inverse problem of reconstructing a lattice set from its discrete X-rays. This problem is of fundamental importance in fields such as image processing [15], statistical data security [10], biplane angiography [12], graph theory [1] and reconstructing crystalline structures from X-rays taken by an electron microscope [11]. For a survey on the state-of-the-art in discrete tomography we suggest the recent book [9].

☆ This work is partially supported by Vigoni project and by PAR University Siena project.

E-mail address: dellungo@unisi.it (A. Del Lungo).

[1] If $k \in \mathbb{N}$, then a $(0,1,\ldots,k)$-matrix is one whose entries all are from $\{0,1,\ldots,k\}$.

0304-3975/02/$ - see front matter
PII: S0304-3975(02)00015-4

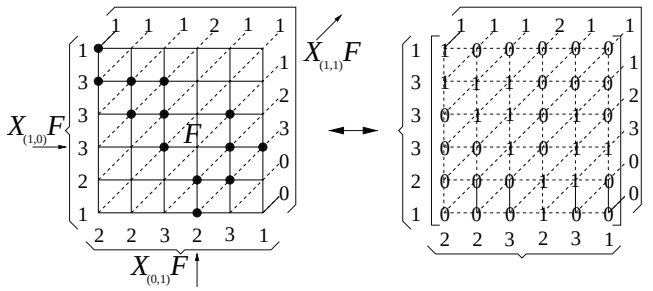


Fig. 1. A lattice set F with the corresponding $(0,1)$-matrix. $X_{(1,0)}F$, $X_{(0,1)}F$ and $X_{(1,1)}F$ are the discrete X-rays in the directions $(1,0)$, $(0,1)$ and $(1,1)$.

A *permutation matrix* A of order n is a $(0,1)$-matrix of size n by n such that $AA^{\mathrm{T}} = A^{\mathrm{T}}A = I_n$, where A^{T} is the transpose of A and I_n denotes the identity matrix of order n. The $n!$ permutation matrices of order n are obtained from I_n by permuting the columns of I_n. The definition implies that a permutation matrix has a single entry "1" in each row and column and all other entries "0". Therefore, the value of its X-ray in horizontal or vertical direction is equal to 1. The values of the X-ray in horizontal and vertical directions are equal to the row and column sums of the matrix, respectively. A sum of k permutation matrices gives a $(0,1,\ldots,k)$-matrix A such that all of the row and column sums of A are equal to k. This is a well-known class of matrices having some interesting combinatorial properties [2].

In [3] the authors study the reconstruction of permutation matrices from their X-rays in some prescribed finite set of directions. They present a first approach to characterizing permutation matrices that are accessible only via their X-rays.

The purpose of this paper is to study the reconstruction of sums of permutation matrices from their X-rays in the diagonal direction $(1,1)$. The X-ray in the direction $(1,1)$ is equal to the diagonal sums of the matrix. From the results proved in [3], it follows that the reconstruction of sums of k permutation matrices from their diagonal sums is $\mathbb{NP}$-complete. We tackle a very simple variant of this problem in which the permutation matrices lie on a cylinder instead of a plane. In this case, quite surprisingly, the problem can be solved in polynomial time. We give an exact, algebraic characterization of the diagonal sums that correspond to a sum of permutation matrices. This means that we provide a necessary and sufficient consistency condition for an integral vector to be the diagonal sums of a sum of permutation matrices. We point out that this condition can be checked in linear time. Moreover, we derive an $O(kn^2)$ time algorithm for reconstructing a sum of k permutation matrices of order n from its diagonal sums. We obtain these results by generalizing a classical theorem of Hall on finite abelian groups [7]. The algorithm follows from the constructive proof of the theorem.

We point out that the characterization of permutation matrices that are accessible only via their X-rays is a project of Maurice Nivat, and this paper arose from several discussions with Maurice on the topic.

2. The planar case

A sum of k permutation matrices of order n gives a matrix $A=(a_{i,j})$ such that $0\leqslant a_{i,j}\leqslant k$ and all the row and column sums of A are equal to k (see Fig. 2). Conversely, if A is a $(0,1,\ldots,k)$-matrix of order n having all its row and column sums equal to k, then there exist k permutation matrices $P_1,\ldots,P_k$ of order n such that $A=P_1+\cdots+P_k$. This result is a corollary of the celebrated Birkhoff–von Neumann Theorem [2, pp. 9,10].

Let $A=(a_{i,j})$ be a sum of k permutation matrices of order n, and let $D=(d_1,d_2,\ldots,d_{2n-1})$ be its diagonal sums. This means that, $d_i=\sum_{h=1}^{i} a_{h,i-h+1}$, for $i=1,\ldots,n$, and $d_{n+i}=\sum_{h=i+1}^{n} a_{h,n+i-h+1}$, for $i=1,\ldots,n-1$. Then D satisfies the following conditions:

$$0 \leqslant d_i \leqslant ki \quad \text{for } i=1,\ldots,n, \tag{2.1}$$

$$0 \leqslant d_{n+i} \leqslant k(n-i) \quad \text{for } i=1,\ldots,n-1, \tag{2.2}$$

$$\sum_{i=1}^{2n-1} d_i = kn. \tag{2.3}$$

Moreover, since $k\sum_{i=1}^{n} i + k\sum_{j=1}^{n} j = \sum_{i+j=k+1}(i+j)\,d_k$, we have

$$\sum_{i=1}^{2n-1} id_i = kn^2. \tag{2.4}$$

We can now introduce the following decision problem on the sum of permutation matrices.

Consistency of the diagonal sums of sums of permutation matrices (DSSPM)

Instance: A vector $D=(d_1,d_2,\ldots,d_{2n-1})$ with integer entries and satisfying conditions (2.1)–(2.4), and a non-negative integer k.

Question: Is there a $(0,1,\ldots,k)$-matrix of order n that has all the row and column sums equal to k and diagonal sums equal to D?

Conditions (2.1)–(2.4) are not sufficient conditions for the existence of a solution of the problem. For example, suppose that $D=(1,0,1,1,0,0,0,1,1)$, with $n=5$ and $k=1$. The vector D satisfies $0\leqslant d_i\leqslant i$, for $i=1,\ldots,5$, $0\leqslant d_{5+i}\leqslant 5-i$, for $i=1,\ldots,4$,

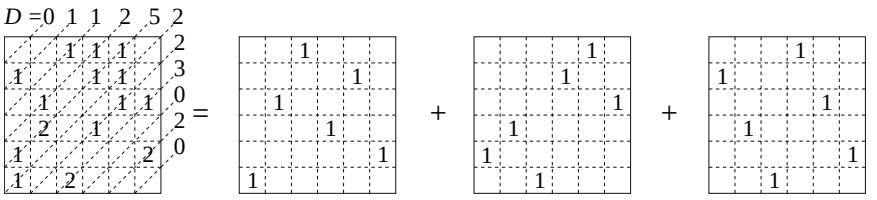


Fig. 2. A sum of three permutation matrices of order 6 and its diagonal sums.

$\sum_{i=1}^{9} d_i = 5$ and $\sum_{i=1}^{9} id_i = 25$ (i.e., D satisfies conditions (2.1)–(2.4)). But there is no a permutation matrix of order 5 that has diagonal sums equal to D.

In [3] it is shown that the previous problem is $\mathbb{NP}$-complete on the class of permutation matrices (i.e., when $k = 1$). From this result it follows that DSSPM is $\mathbb{NP}$-complete.

3. The cylindrical case

We now consider a simple variant of DSSPM in which the permutation matrices belong to a cylinder instead to a plane (see Fig. 3(b)).

Let $A = (a_{i,j})$ be a sum of k permutation matrices of order n, and let $D = (d_1, d_2, \ldots, d_{2n-1})$ be its diagonal sums. By connecting the two opposite vertical sides of A as shown in Fig. 3, we obtain a sum of k permutation matrices $\bar{A}$ that lie on a cylinder. The diagonal sums of $\bar{A}$ are given by a vector $\bar{D} = (\bar{d_1}, \bar{d_2}, \ldots \bar{d_n})$ such that $\bar{d_i} = d_i + d_{n+i}$ for $1 \leqslant i < n$, and $\bar{d_n} = d_n$. We also say that $\bar{D}$ is the *cylindrical* diagonal sums of A.

From conditions (2.1)–(2.3) we deduce that the cylindrical diagonal sums $\bar{D}$ satisfy

$$0 \leqslant \bar{d}_i \leqslant kn \quad \text{for } i = 1, 2, \ldots, n, \tag{3.1}$$

$$\sum_{i=1}^{n} \bar{d}_i = kn. \tag{3.2}$$

Moreover, $\sum_{i=1}^{n} i\bar{d_i} = \sum_{i=1}^{2n-1} id_i - n\sum_{i=1}^{n-1} d_{n+i}$, and so by condition (2.4): $\sum_{i=1}^{n} i\bar{d_i} = n(kn - \sum_{i=1}^{n-1} d_{n+i})$. From condition (2.3) it follows that $kn - \sum_{i=1}^{n-1} d_{n+i} = \sum_{i=1}^{n} d_i$. Thus

$$\sum_{i=1}^{n} i\bar{d}_i = \delta n, \tag{3.3}$$

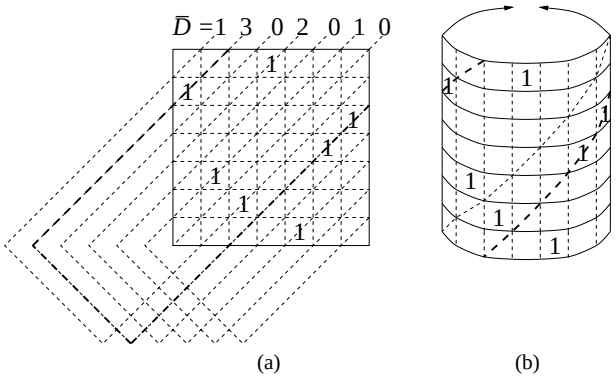


Fig. 3. (a) A permutation matrix A and its cylindrical diagonal sums. (b) Its corresponding permutation matrix $\bar{A}$ on a cylinder.

where δ is an integer number such that $k \leqslant \delta \leqslant kn$, and it gives the sum of entries in the first n diagonals of A (i.e., $\delta = \sum_{i=1}^{n} d_i$).

We can now define *Consistency of the Diagonal Sums of Sums of Permutation Matrices* (CDSSPM) assuming that the permutation matrices are on a cylinder.

Consistency of the cylindrical diagonal sums of sums of permutation matrices (CDSSPM)

Instance: A vector $\bar{D} = (\bar{d_1}, \bar{d_2}, \ldots, \bar{d_n})$ with integer entries and satisfying conditions (3.1)–(3.3), and a non-negative integer k.

Question: Is there a $(0, 1, \ldots, k)$-matrix of order n that has all the row and column sums equal to k and cylindrical diagonal sums equal to $\bar{D}$?

Quite surprisingly, conditions (3.1)–(3.3) imply the existence of a solution to this decision problem. Therefore, we have three necessary and sufficient consistency conditions for an integral vector to be the diagonal sums of a sum of permutation matrices, and we claim we can check these conditions in linear time. We prove this claim by proving a generalization of a classical theorem of Hall on the finite abelian groups [9]. We begin by reducing CDSSPM to the following decision numerical matching problem on the additive group of integers modulo n (i.e., $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$).

Numerical matching on $\mathbb{Z}_n$

Instance: A non-negative integer k, and a multiset $C = \{c_1, c_2 \ldots, c_{kn}\}$ of $\mathbb{Z}_n$.

Question: Are there k permutations $\pi_1, \ldots, \pi_k$ of the elements of $\mathbb{Z}_n$ such that

$$i - 1 + \pi_h(i-1) \equiv c_{h,i} \,(\mathrm{mod}\, n) \quad \text{for } i = 1, \ldots, n,\ h = 1, \ldots, k, \tag{3.4}$$

where $\{c_{i,h} : 1 \leqslant i \leqslant n,\ 1 \leqslant h \leqslant k\} = C$?

Lemma 3.1. *There is a linear transformation from CDSSPM to numerical matching on $\mathbb{Z}_n$.*

Proof. Given an instance $\bar{D} = (\bar{d_1}, \ldots, \bar{d_n})$ of the first problem, we determine a multiset $C = \{c_1, \ldots, c_{kn}\}$ such that

$$\begin{aligned} &c_1 = \cdots = c_{\bar{d_1}} = 0, \\ &c_{\bar{d_1}+1} = \cdots = c_{\bar{d_1}+\bar{d_2}} = 1, \ldots, c_{\bar{d_1}+\cdots+\bar{d}_{n-1}+1} = \cdots = c_{kn} = n-1. \end{aligned} \tag{3.5}$$

By conditions (3.1) and (3.2), the multiset $C = \{c_1, \ldots, c_{kn}\}$ is an instance of numerical matching on $\mathbb{Z}_n$. We prove that there exists a $(0, 1, \ldots, k)$-matrix A of order n that has all the row and column sums equal to k and cylindrical diagonal sums equal to $\bar{D}$ if and only if there exist k permutations $\pi_1, \ldots, \pi_k$ of the elements of $\mathbb{Z}_n$ satisfying condition (3.4).

Let us suppose that there is a $(0, 1, \ldots, k)$-matrix A of order n that has all the row and column sums equal to k and cylindrical diagonal sums equal to $\bar{D}$. There are k permutation matrices $P_1 = (p_{i,j}^{(1)}), \ldots, P_k = (p_{i,j}^{(k)})$ of order n such that $A = P_1 + \cdots + P_k$.

Let $B_h = \{(1, j_1), (2, j_2), \ldots, (n, j_n)\}$ be the set of pair such that $p^{(h)}_{i,j_i} = 1$. By setting $\pi_h(i-1) = j_i - 1$, for $i = 1, \ldots, n$, we obtain that π_h is a permutation of $\{0, 1, \ldots, n-1\}$.

From $A = P_1 + \cdots + P_k$, it follows that $\bar{D} = \bar{D}_1 + \cdots + \bar{D}_k$, where $\bar{D}_h$ is the cylindrical diagonal sums of the permutation matrix P_h, for $h = 1, \ldots, k$. Since $\bar{D}_h = (\bar{d}^{(h)}_1, \ldots, \bar{d}^{(h)}_n)$ is the sequence of cylindrical diagonal sums of P_h, there are $\bar{d}^{(h)}_i$ distinct pairs (l, j_l) of B_h such that

$$l + j_l = i + 1 \text{ or } l + j_l = n + i + 1,$$

for each $i = 1, \ldots, n$. By the definition of π_h,

$$l - 1 + \pi_h(l-1) = i - 1 \text{ or } l - 1 + \pi_h(l-1) = n + i - 1,$$

that is

$$l - 1 + \pi_h(l-1) \equiv i - 1 \,(\mathrm{mod}\, n).$$

Therefore, for each $h = 1, \ldots, k$, there is a set $L_h \subset \{1, \ldots, n\}$ such that $|L_h| = \bar{d}^{(h)}_i$ and

$$l - 1 + \pi_h(l-1) \equiv i - 1 \,(\mathrm{mod}\, n), \quad \forall l \in L_h. \tag{3.6}$$

By this relation, $\pi_1, \ldots, \pi_k$ is a solution for C of the matching problem. In fact, $\bar{d}_i = \bar{d}^{(1)}_i + \cdots + \bar{d}^{(k)}_i$ and C contains $\bar{d}_i$ elements equal to $i - 1$.

Conversely, let $\pi_1, \ldots, \pi_k$ be k permutations of the elements of $\mathbb{Z}_n$ satisfying condition (3.4). By the definition of C, for each $i = 1, \ldots, n$, there are k subsets $L_1, \ldots, L_k$ of $\{1, \ldots, n\}$ such that L_h satisfies condition (3.6), $|L_h| = \bar{d}^{(h)}_i$, for $h = 1, \ldots, k$, and $\bar{d}_i = \bar{d}^{(1)}_i + \cdots + \bar{d}^{(k)}_i$. Therefore, for each $h = 1, \ldots, k$, there are $\bar{d}^{(h)}_i$ distinct pairs $(l, \pi_h(l-1) + 1)$ such that

$$l + \pi_h(l-1) + 1 = i + 1 \text{ or } l + \pi_h(l-1) + 1 = n + i + 1.$$

Consequently, the matrix $P_h = (p^{(h)}_{i,j})$ having $p^{(h)}_{l,\pi_h(l-1)+1} = 1$, for $l = 1, \ldots, n$, and all other entries 0, is a permutation matrix of order n and its ith cylindrical diagonal sum is equal to $\bar{d}^{(h)}_i$. Since $\bar{d}_i = \bar{d}^{(1)}_i + \cdots + \bar{d}^{(k)}_i$, we have that the matrix $A = P_1 + \cdots + P_k$ has all the row and column sums equal to k and ith cylindrical diagonal sums equal to $\bar{d}_i$. □

From this lemma it follows that, if *Numerical Matching on* $\mathbb{Z}_n$ can be solved in polynomial time, then CDSSPM can be solved in the same computational time. Now, by using a classical theorem of Hall [7], we show that if the non-negative integer k of the instance is equal to 1, then this decision matching problem is solvable in linear time.

Let G be a finite abelian group of order n. Let $\mathscr{M}_i$ denote the class of multisets of G of size i.

Theorem 3.2 (Hall [7]). *If G is a finite abelian group of order n, and $C \in \mathscr{M}_n$, then there exists a permutation π of the elements of G such that $C = \{a + \pi(a) : a \in G\}$ if*

and only if

$$\sum_{c\in C} c = 0. \tag{3.7}$$

Remark. This result was rediscovered by Salzborn and Szekeres [13], where they proved the following equivalent of Hall's Theorem:

- If $C\in\mathscr{M}_{n-1}$, then there exists a permutation π of the elements of G and an element g of G such that $C=\{a+\pi(a): a\in G\setminus\{g\}\}$.

Their proof is different from Hall's, but it is at the same "level" and "difficulty". These are constructive proofs of this result that give an algorithm to find a permutation π satisfying the statement of the theorem in time $O(n^2)$.

We point out that the theorem states that condition (3.7) is a necessary and sufficient consistency condition for the existence of a permutation π of the elements of G such that $C=\{a+\pi(a): a\in G\}$. Therefore, we can establish the existence of this permutation in linear time. However, if we want to construct such a permutation, then we have to perform the algorithm deduced by one of the constructive proofs of the theorem, and these algorithms have computational complexity $O(n^2)$.

The additive group $\mathbb{Z}_n$ is a finite abelian group of order n and so by Hall's Theorem, if $k=1$, there exists a solution of numerical matching on $\mathbb{Z}_n$ if and only if the instance C satisfies condition (3.7) (i.e., $\sum_{i=1}^{n} c_i = 0$ on $\mathbb{Z}_n$). Since we can check this condition in linear time, we obtain that, if $k=1$, the decision matching problem can be solved in linear time, and so Lemma 3.1 establishes that CDSSPM can be also solvable in linear time.

By proceeding in a similar fashion, we deduce that CDSSPM can be solved in linear time for each $k\geqslant 1$, if we are able to prove the following generalization of Hall's Theorem.

Theorem 3.3. *If G is a finite abelian group of order n, and $C\in\mathscr{M}_{kn}$, where k is a positive integer number, then there exist k permutations $\pi_1,\ldots,\pi_k$ of the elements of G such that*

$$C=\{a+\pi_i(a): a\in G, 1\leqslant i\leqslant k\} \tag{3.8}$$

if and only if

$$\sum_{c\in C} c = 0. \tag{3.9}$$

Condition (3.9) is necessary for the existence of k permutations $\pi_1,\ldots,\pi_k$ of G satisfying condition (3.8). The theorem can be proved by using a result from combinatorial group theory. We introduce a definition which allows us to present this theorem.

The *Davenport constant* $D(G)$ of G is the least integer d such that for any $C\in\mathscr{M}_d$ there is $K\subset C$ such that $\sum_{c\in K} c=0$.

Theorem 3.4. *Let G be a finite abelian group of order n. If $C\in\mathscr{M}_m$, with $m\geqslant n+D(G)-1$, then there is $K\subset C$ such that $|K|=n$ and $\sum_{c\in K} c=0$.*

Remark. This theorem has been proved by Gao [6] in 1996 and some generalizations can be found in [4,8]. This theorem belongs to "Zero-Sum Ramsey Theory" which is a newly established area of combinatorics. The paradigm of zero-sum problems is the following:

- suppose the elements of a combinatorial structure are mapped into a finite group G. Does there exists a prescribed substructure such that the sum of the weights of its elements is 0 in G?

A survey of Zero-Sum Ramsey Theory is given in [5], and a recent result can be found in [14].

Proof of Theorem 3.3. Since $D(G) \leqslant n$, it follows from Theorem 3.4 that for any $C \in \mathscr{M}_{2n-1}$ there is $K \subset C$ such that $|K| = n$ and $\sum_{c \in K} c = 0$. Consequently, every $C \in \mathscr{M}_{kn}$ with $\sum_{c \in C} c = 0$ can be split into k subsets each of size n, and each of which also sums to 0. Theorem 3.3 follows from this result and Hall's Theorem. □

By Theorem 3.3, there exists a solution of numerical matching on $\mathbb{Z}_n$ if and only if its instance C satisfies condition (3.9). Consequently, the matching problem can be solved in linear time, and so CDSSPM can be also solved in linear time.

Moreover, condition (3.9) for the instance $C = \{c_1, \ldots, c_{kn}\}$ corresponds to condition (3.3) for the instance $\bar{D} = (\bar{d}_1, \bar{d}_2, \ldots, \bar{d}_n)$. In fact, by the definition of C,

$$\sum_{i=1}^{kn} c_i = \sum_{i=1}^{n} (i-1)\bar{d}_i,$$

and by condition (3.2) we deduce that $\sum_{i=1}^{kn} c_i = 0$ on $\mathbb{Z}_n$ if and only if $\sum_{i=1}^{n} i\bar{d}_i = \delta n$, where δ is an integer number such that $k \leqslant \delta \leqslant kn$. Therefore:

Theorem 3.5. *There is a $(0, 1, \ldots, k)$-matrix of order n that has all the row and column sums equal to k, and cylindrical diagonal sums equal to $\bar{D} = (\bar{d}_1, \bar{d}_2, \ldots, \bar{d}_n)$ if and only if $\bar{D}$ satisfies conditions* (3.1)–(3.3).

3.1. The reconstruction problem

Now we tackle the problem of reconstructing a $(0, 1, \ldots, k)$-matrix of order n from its cylindrical diagonal sums, given that its row and column sums all equal k. That is, given a vector $\bar{D} = (\bar{d}_1, \bar{d}_2, \ldots, \bar{d}_n)$ that satisfies conditions (3.1)–(3.3), we want to reconstruct a $(0, 1, \ldots, k)$-matrix of order n that has all its row and column sums equal to k, and its cylindrical diagonal sums equal to $\bar{D}$.

Suppose a multiset C of $\mathscr{M}_{kn}$ satisfying condition (3.9) is given. If we are able to provide a polynomial-time algorithm for determining k permutations $\pi_1, \ldots, \pi_k$ of G satisfying condition (3.8), then we can determine a solution of numerical matching on $\mathbb{Z}_n$ in polynomial time. So, if we are able to devise this algorithm, then the proof of Lemma 3.1 gives a procedure for reconstructing a $(0, 1, \ldots, k)$-matrix from its cylindrical diagonal sums.

Since the existing proofs of Theorem 3.4 are not constructive, we propose an alternative, direct and constructive proof of Theorem 3.3. This proof provides an efficient

algorithm for determining the k permutations $\pi_1, \ldots, \pi_k$ of G satisfying condition (3.8).

An alternative and constructive proof of Theorem 3.3. We introduce the following notation and definitions:

- $\mathscr{M}_k^0$ is the set of the multisets G of size k and sum 0;
- $\mathscr{S}$ is the group of permutations of G;
- $\mathscr{T} = \mathscr{S} \times G$ is the set of "tagged permutations" of G;
- for $\pi \in \mathscr{S}, g \in G$ (i.e., $(\pi, g) \in \mathscr{T}$) and $C \in \mathscr{M}_n$ write

$$\pi \vdash C \text{ if } C = \{a + \pi(a) : a \in G\}$$

$$(\pi, g) \vdash C \text{ if } C = \{a + \pi(a) : a \in G \backslash \{g\}\}.$$

Using this notation, Hall's Theorem can be formulated as follows:

$$\forall C \in \mathscr{M}_n : (\exists \pi \in \mathscr{S} : \pi \vdash C) \Leftrightarrow C \in \mathscr{M}_n^0$$

and the equivalent formulation of Salzborn and Szekeres (see the remark after Theorem 3.2) becomes

$$\forall C \in \mathscr{M}_{n-1}\, \exists (\pi, g) \in \mathscr{T} : (\pi, g) \vdash C.$$

We now define a *transition system* on $\mathscr{T}$:

- for $(\pi, g), (\pi', g') \in \mathscr{T}$ and $(c, d) \in G \times G$ write $(\pi, g) \overset{(c,d)}{\to} (\pi', g')$ if

$$\pi' = \pi \circ (\pi(g), \pi(g')), \quad g + \pi(g') = c, \quad g' + \pi(g') = d,$$

  (i.e., π and π' differ just by exchanging the values taken for g and g' (provided $g \neq g'$)).
- if $g = g'$ (or equivalently $c = d$ or $\pi = \pi'$), we have a *degenerate* transition.

Notice that,

- if $(\pi, g) \vdash C \in \mathscr{M}_{n-1}$ and $(\pi, g) \overset{(c,c)}{\to} (\pi, g)$ (i.e., a degenerate transition), then $\pi \vdash C \cup \{c\} \in \mathscr{M}_n^0$.

The main tool of the proof is the following concept of a *coupled system*: Let $\mathscr{A}, \mathscr{B}$ be two copies of $\mathscr{T}$ that will interact by sending each other "messages" (i.e., elements from G) in an alternating way:

- if $\mathscr{A}$ is in state (α, a) and receives c from $\mathscr{B}$, it performs the transition $(\alpha, a) \overset{(c,d)}{\to} (\alpha', a')$ and sends d to $\mathscr{B}$;
- if $\mathscr{B}$ is in state (β, b) and receives d from $\mathscr{A}$, it performs the transition $(\beta, b) \overset{(d,c')}{\to} (\beta', b')$ and sends c' to $\mathscr{A}$;
- initially $\mathscr{A}$ is in state (α_0, a_0) and $\mathscr{B}$ is in state (β_0, b_0) and $\mathscr{A}$ receives $c_0 \in G$.

This process generates transition sequences

$$\text{in } \mathscr{A}\text{: } (\alpha_0,a_0)\overset{(c_0,d_0)}{\to}(\alpha_1,a_1)\overset{(c_1,d_1)}{\to}(\alpha_2,a_2)\overset{(c_2,d_2)}{\to}\cdots$$

$$\text{in } \mathscr{B}\text{: } (\beta_0,b_0)\overset{(d_0,c_1)}{\to}(\beta_1,b_1)\overset{(d_1,c_2)}{\to}(\beta_2,b_2)\overset{(d_2,c_3)}{\to}\cdots\ .$$

We have the following properties. Let $A_j,B_j\in\mathscr{M}_{n-1}$ with $(\alpha_j,a_j)\vdash A_j$ and $(\beta_j,b_j)\vdash B_j$. Then

$$A_{j+1}=(A_j\backslash\{d_j\})\cup\{c_j\},\quad B_{j+1}=(B_j\backslash\{c_{j+1}\})\cup\{d_j\}.$$

From these relations it is easy to deduce that

$$a_{j+1}=a_j+d_j-c_j,\quad b_{j+1}=b_j+c_{j+1}-d_j. \tag{3.10}$$

The process ends when it produces a degenerate transition (i.e., $(\alpha_i,a_i)\overset{(c_i,c_i)}{\to}(\alpha_i,a_i)$ or $(\beta_i,b_i)\overset{(d_i,d_i)}{\to}(\beta_i,b_i)$). Hence either the coupled system produces a degenerate transition or the process continues indefinitely. We show that this second alternative cannot arise. Assume that the process continues indefinitely. Since $a_0,\dots,a_j$ and $b_1,\dots,b_j$ are chosen from the finite group G, we have two possibilities:

1. there exist i and j such that $j\geqslant i$, $a_0,\dots,a_i,\dots,a_j$ are all distinct, $b_0,\dots,b_j$ are all distinct, but $a_{j+1}=a_i$;
2. there exist i and j such that $j\geqslant i$, $a_0,\dots,a_{j+1}$ are all distinct, $b_1,\dots,b_i,\dots,b_j$ are all distinct, but $b_{j+1}=b_i$;

In the first case, by relation (3.10), $a_{j+1}=a_i+d_i-c_i$. Since $a_{j+1}=a_i$ we have $d_i=c_i$, and so by sending the $(2i)$th "message" we obtain $(\alpha_i,a_i)\overset{(c_i,c_i)}{\to}(\alpha_i,a_i)$ and the process ends.

In the second one, by relation (3.10), $b_{j+1}=b_i+c_{i+1}-d_i$. Since $b_{j+1}=b_i$ we have $c_{i+1}=d_i$, and so by sending the $(2i+1)$th "message" we obtain $(\beta_i,b_i)\overset{(d_i,d_i)}{\to}(\beta_i,b_i)$ and the process ends.

Consequently, the coupled system produces a degenerate transition in i steps, with $i<n$. More precisely:

Lemma 3.6. *Let $(\alpha_0,a_0)\vdash A_0$, $(\beta_0,b_0)\vdash B_0$, $c_0\in G$ be a starting position of the coupled system. Then there exists an integer $i<n$ such that $\alpha_i\vdash A_i\cup\{c_i\}\in\mathscr{M}_n^0$ or $\beta_i\vdash B_i\cup\{d_i\}\in\mathscr{M}_n^0$.*

This lemma allows us to prove Theorem 3.3:

Let M be the set of the first $2n-1$ elements of a multiset $C\in\mathscr{M}_{kn}^0$ (i.e., C satisfies condition (3.9)). We have that $M=A_0\cup B_0\cup\{c_0\}$, where $A_0,B_0\in\mathscr{M}_{n-1}$, $c_0\in G$. By Hall's Theorem, there exist $(\alpha_0,a_0),(\beta_0,a_0)\in\mathscr{T}$ such that $(\alpha_0,a_0)\vdash A_0$ and $(\beta_0,b_0)\vdash B_0$. By Lemma 3.6, there exists $i<n$ such that $\alpha_i\vdash A_i\cup\{c_i\}\in\mathscr{M}_n^0$ or $\beta_i\vdash B_i\cup\{d_i\}\in\mathscr{M}_n^0$. If $\alpha_i\vdash A_i\cup\{c_i\}$, then set $C_1=A_i\cup\{c_i\}$ and $\pi_1=\alpha_i$, else set $C_1=B_i\cup\{c_i\}$ and $\pi_1=\beta_i$. Since $\pi_1\vdash C_1\in\mathscr{M}_n^0$ and $C\in M_{kn}^0$, we have that $C'=C\backslash C_1\in M_{(k-1)n}^0$. Therefore, by repeating the procedure recursively on C', we obtain k permutations $\pi_1,\dots,\pi_k$ of

G such that $\pi_1 \vdash C_1 \in \mathscr{M}_n^0, \ldots, \pi_k \vdash C_k \in \mathscr{M}_n^0$, with $C = C_1 \cup \cdots \cup C_k$. This means that $\pi_1, \ldots, \pi_k$ satisfy condition (3.8) of Theorem 3.3. □

This direct proof of Theorem 3.3 provides an algorithm which finds k permutations $\pi_1, \ldots, \pi_k$ of G satisfying condition (3.8). The algorithm performs the procedure described in the proof of the theorem $k-1$ times. At first this procedure finds $(\alpha_0, a_0), (\beta_0, a_0) \in \mathscr{T}$ such that $(\alpha_0, a_0) \vdash A_0$ and $(\beta_0, b_0) \vdash B_0$ in $O(n^2)$ time, by using the algorithm deduced by the proof of Hall's Theorem. Then, by running the coupled system it achieves a degenerate transition $\pi_1 \vdash C_1 \in \mathscr{M}_n^0$ in $O(n)$ time. Therefore, the computational complexity of the procedure is $O(n^2)$. Consequently, we are able to determine a solution of numerical matching on $\mathbb{Z}_n$ in time $O(kn^2)$.

Example 3.7. Assume that the abelian group $G = \mathbb{Z}_n$, with $n = 6$. The multiset $C = \{4,3,3,0,3,5,2,5,1,4,3,4,1,1,4,1,4,0\} \in \mathscr{M}_{18}^0$. In fact, it is a sequence of 18 elements of $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$, $k = 3$, and C satisfies condition (3.8) (the sum of its elements is $48 \equiv 0 \pmod 6$). We take the first $2n-1 = 11$ elements and we set $A_0 = \{4,3,3,0,3\}, B_0 = \{5,2,5,1,4\}$ and $c_0 = 3$. By performing the algorithm deduced by the proof of Hall's Theorem on A_0 and B_0, we find $(\alpha_0, a_0) \vdash A_0$ and $(\beta_0, b_0) \vdash B_0$, where

$$\alpha_0 = (4,2,1,3,5,\mathbf{0}), \quad a_0 = 5, \quad \beta_0 = (5,1,3,4,0,\mathbf{2}), \quad b_0 = 5.$$

Then we run the coupled system:

$$\begin{aligned}
&(\alpha_0, a_0) \overset{(c_0,d_0)}{\to} (\alpha_1, a_1), \text{ where } \alpha_1 = (\mathbf{0},2,1,3,5,4),\ a_1 = 0,\ d_0 = 4,\ A_1 = \{3,3,0,3,3\},\\
&(\beta_0, b_0) \overset{(d_0,c_1)}{\to} (\beta_1, b_1), \text{ where } \beta_1 = (\mathbf{2},1,3,4,0,5),\ b_1 = 0,\ c_1 = 5,\ B_1 = \{2,5,1,4,4\},\\
&(\alpha_1, a_1) \overset{(c_1,d_1)}{\to} (\alpha_2, a_2), \text{ where } \alpha_2 = (5,2,1,3,\mathbf{0},4),\ a_2 = 4,\ d_1 = 3,\ A_2 = \{5,3,3,0,3\},\\
&(\beta_1, b_1) \overset{(d_1,c_2)}{\to} (\beta_2, b_2), \text{ where } \beta_2 = (3,1,\mathbf{2},4,0,5),\ b_2 = 2,\ c_2 = 5,\ B_2 = \{3,2,1,4,4\},\\
&(\alpha_2, a_2) \overset{(c_2,d_2)}{\to} (\alpha_3, a_3), \text{ where } \alpha_3 = (5,2,\mathbf{0},3,1,4),\ a_3 = \mathbf{2},\ d_2 = 3,\ A_3 = \{5,3,0,5,3\},\\
&(\beta_2, b_2) \overset{(d_2,c_3)}{\to} (\beta_3, b_3), \text{ where } \beta_3 = (3,\mathbf{2},1,4,0,5),\ b_3 = 1,\ c_3 = \mathbf{2},\ B_3 = \{3,3,1,4,4\},\\
&(\alpha_3, a_3) \overset{(c_3,d_3)}{\to} (\alpha_4, a_4), \text{ where } \alpha_4 = \alpha_3 \qquad\qquad a_4 = \mathbf{2},\ d_3 = \mathbf{2},\ A_4 = A_3.
\end{aligned}$$

The coupled system produces a degenerate transition $(\alpha_3, a_3) \overset{(c_3,c_3)}{\to} (\alpha_3, a_3)$ and the process ends. Therefore, $\alpha_3 \vdash A_3 \cup \{c_3\} = \{5,3,0,5,3,2\} \in \mathscr{M}_6^0$ and we set $C_1 = A_3 \cup \{c_3\}$, $\pi_1 = \alpha_3$, and $C' = C \setminus C_1 = \{3,3,1,4,4,4,1,1,4,1,4,0\} \in \mathscr{M}_{12}^0$.

Now, we repeat the procedure on C'. We take the first $2n-1 = 11$ elements and we set $A_0 = \{3,3,1,4,4\}, B_0 = \{4,1,1,4,1\}$ and $c_0 = 4$. Since A_0 is equal to the previous B_3, we have that $(\alpha_0, a_0) \vdash A_0$ where

$$\alpha_0 = (3,\mathbf{2},1,4,0,5), \quad a_0 = 1.$$

So, we perform Hall's algorithm only on B_0. We find $(\beta_0, b_0) \vdash B_0$, where

$$\beta_0 = (4,0,5,1,3,\mathbf{2}), \quad b_0 = 5.$$

Then we run the coupled system:

$$
\begin{aligned}
&(\alpha_0,a_0)\overset{(c_0,d_0)}{\to}(\alpha_1,a_1),\ \text{where}\ \alpha_1=(\mathbf{2},3,1,4,0,5),\ a_1=0,\ d_0=3,\ A_1=\{4,3,1,4,4\},\\
&(\beta_0,b_0)\overset{(d_0,c_1)}{\to}(\beta_1,b_1),\ \text{where}\ \beta_1=(\mathbf{2},0,5,1,3,4),\ b_1=0,\ c_1=4,\ B_1=\{1,1,4,1,3\},\\
&(\alpha_1,a_1)\overset{(c_1,d_1)}{\to}(\alpha_2,a_2),\ \text{where}\ \alpha_2=(4,3,1,\mathbf{2},0,5),\ a_2=3,\ d_1=1,\ A_2=\{4,4,3,4,4\},\\
&(\beta_1,b_1)\overset{(d_1,c_2)}{\to}(\beta_2,b_2),\ \text{where}\ \beta_2=(1,0,5,\mathbf{2},3,4),\ b_2=3,\ c_2=4,\ B_2=\{1,1,1,1,3\},\\
&(\alpha_2,a_2)\overset{(c_2,d_2)}{\to}(\alpha_3,a_3),\ \text{where}\ \alpha_3=(4,3,\mathbf{2},1,0,5),\ a_3=2,\ d_2=3,\ A_3=\{4,4,4,4,4\},\\
&(\beta_2,b_2)\overset{(d_2,c_3)}{\to}(\beta_3,b_3),\ \text{where}\ \beta_3=(1,\mathbf{2},5,0,3,4),\ b_3=1,\ c_3=1,\ B_3=\{1,1,3,1,3\},\\
&(\alpha_3,a_3)\overset{(c_3,d_3)}{\to}(\alpha_4,a_4),\ \text{where}\ \alpha_4=(4,3,5,1,0,\mathbf{2}),\ a_4=\mathbf{5},\ d_3=4,\ A_4=\{4,4,1,4,4\},\\
&(\beta_3,b_3)\overset{(d_3,c_4)}{\to}(\beta_4,b_4),\ \text{where}\ \beta_4=(1,3,5,0,\mathbf{2},4),\ b_4=4,\ c_4=\mathbf{1},\ B_4=\{1,4,1,3,3\},\\
&(\alpha_4,a_4)\overset{(c_4,d_4)}{\to}(\alpha_5,a_5),\ \text{where}\ \alpha_5=\alpha_4\qquad\qquad a_5=\mathbf{5},\ d_4=\mathbf{1},\ A_5=A_4.
\end{aligned}
$$

The coupled system produces a degenerate transition $(\alpha_4,a_4)\overset{(c_4,c_4)}{\to}(\alpha_4,a_4)$ and the process ends. Therefore, $\alpha_4\vdash A_4\cup\{c_4\}=\{4,4,1,4,4,1\}\in\mathscr{M}_6^0$ and we set $C_2=A_3\cup\{c_3\}$, $\pi_2=\alpha_3$, and $C''=C'\backslash C_2=\{1,4,1,3,3,0\}\in M_6^0$. Since $C''=B_4\cup\{0\}$, we have that $\beta_4\vdash C''$. We set $C_3=C''$ and $\pi_3=\beta_4$. Therefore, the algorithm provides three permutations

$$\pi_1=(5,2,0,3,1,4),\quad \pi_2=(4,3,5,1,0,2),\quad \pi_3=(1,3,5,0,2,4)$$

such that $\pi_1\vdash C_1,\pi_2\vdash C_2,\pi_3\vdash C_3$, with $C=C_1\cup C_2\cup C_3$. This means that π_1,π_2,π_3 is a solution for the instance C of numerical matching on $\mathbb{Z}_6$.

From the previous algorithm and the proof of Lemma 3.1, it follows that:

Theorem 3.8. *Let* $\bar{D}=(\bar{d_1},\ldots,\bar{d_n})$ *be a vector satisfying conditions* (3.1), (3.2) *and* (3.3). *We can reconstruct a* $(0,1,\ldots,k)$*-matrix of order n that has all the row and column sums equal to k, and cylindrical diagonal sums equal to* $\bar{D}$ *in time* $O(kn^2)$.

The basic steps of this reconstruction algorithm are the following: given an instance $\bar{D}=(\bar{d_1},\ldots,\bar{d_n})$ satisfying conditions (3.1)–(3.3), we determine the multiset $C=\{c_1,\ldots,c_{kn}\}$ satisfying condition (3.8). Then, we perform the previous algorithm which finds a solution $\pi_1,\ldots,\pi_k$ for C of the matching problem. We define the permutation matrix $P_h=(p_{i,j}^{(h)})$ that has $p_{i,\pi_h(i-1)+1}^{(h)}=1$, for $i=1,\ldots,n$, and all other entries 0, for each $h=1,\ldots,k$. Finally, the matrix $A=P_1+\cdots+P_k$ is a $(0,1,\ldots,k)$-matrix of order n that has all the row and column sums equal to k and cylindrical diagonal sums $\bar{D}$.

For instance, if $\bar{D}=(2,4,1,4,5,2)$, we determine $C=\{0,0,1,1,1,1,2,3,3,3,3,4,4,4,4,4,5,5\}$. The previous example gives the solution $\pi_1=(5,2,0,3,1,4)$, $\pi_2=(4,3,5,1,0,2)$, $\pi_3=(1,3,5,0,2,4)$ for C. Thus, the permutation matrices $P_1=(p_{i,j}^{(1)}),P_2=(p_{i,j}^{(2)})$ and $P_3=(p_{i,j}^{(3)})$ are such that:

$$p_{1,6}^{(1)}=p_{2,3}^{(1)}=p_{3,1}^{(1)}=p_{4,4}^{(1)}=p_{5,2}^{(1)}=1,\ p_{6,5}^{(1)}=1,$$

$$p_{1,5}^{(2)}=p_{2,4}^{(2)}=p_{3,6}^{(1)}=p_{4,2}^{(2)}=p_{5,1}^{(2)}=1,\ p_{6,3}^{(2)}=1,$$

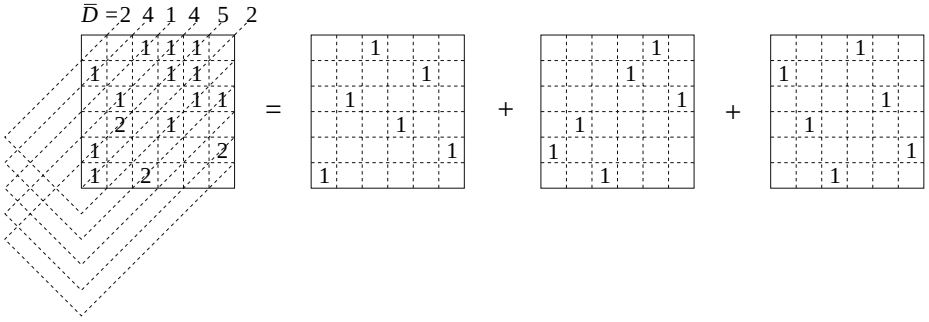


Fig. 4. A sum of three permutation matrices of order 6 and its cylindrical diagonal sums.

$$p^{(3)}_{1,2} = p^{(3)}_{2,4} = p^{(3)}_{3,6} = p^{(3)}_{4,1} = p^{(2)}_{5,3} = 1, \;\; p^{(3)}_{6,5} = 1,$$

and all other entries 0. Therefore, the matrix $A = P_1 + P_2 + P_3$ is a $(0,1,2,3)$-matrix that has all the row and column sums equal to 3 and cylindrical diagonal sums $\bar{D} = (2,4,1,4,5,2)$ (see Fig. 4).

3.2. Conjecture for CDSSPM on the class of (0,1)-matrices

In this subsection we tackle CDSSPM on the class of $(0,1)$-matrices. Given a vector $\bar{D} = (\bar{d}_1, \bar{d}_2, \ldots, \bar{d}_n)$ with integer entries, we have to establish the existence of a $(0,1)$-matrix of order n that has all the row and column sums equal to k and cylindrical diagonal sums equal to $\bar{D}$.

The Birkhoff–von Neumann Theorem [2, pp. 9 and 10] provides an interesting decomposition property for those $(0,1,\ldots,k)$-matrices of order n having all the row and column sums equal to k (see Section 2), which implies that if A is a $(0,1)$-matrix of order n all of whose row and column sums are equal to the positive integer k, then there exist k permutation matrices $P_1, \ldots, P_k$ of order n such that $A = P_1 + \cdots + P_k$. From this decomposition, we deduce that CDSSPM applied to the class of $(0,1)$-matrices could give a result similar to Theorem 3.5.

Let $\bar{D} = (\bar{d}_1, \ldots, \bar{d}_n)$ be the cylindrical diagonal sums of a $(0,1)$-matrix of order n such that all row and column sums are equal to k. The vector $\bar{D}$ satisfies conditions (3.2), (3.3), and

$$0 \leqslant \bar{d}_i \leqslant n, \quad \text{for } i = 1, \ldots, n, \tag{3.11}$$

instead of conditions (3.1). Therefore, condition (3.11) is necessary for the existence of a $(0,1)$-matrix of order n having all the row and column sums equal to k, and cylindrical diagonal sums $\bar{D}$.

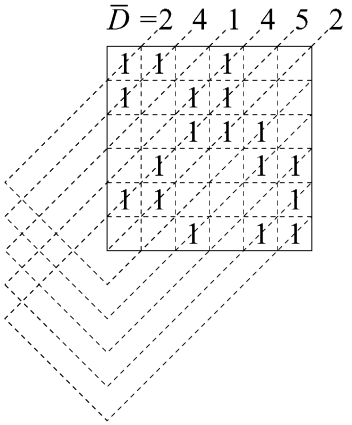
Condition (3.11) implies conditions (3.1), and so by Theorem 3.5, if $\bar{D}$ satisfies conditions (3.11), (3.2) and (3.3), there is at least one $(0,1,\ldots,k)$-matrix of order n that has all the row and column sums equal to k, and cylindrical diagonal sums equal to $\bar{D}$. Now, we have to answer the following question:

- does this family of $(0,1,\ldots,k)$-matrices contain at least one $(0,1)$-matrix?

Maurice Nivat and I feel that conditions (3.11), (3.2) and (3.3), imply the existence of such $(0,1)$-matrix. This means that

Conjecture 3.9. *There is a* $(0,1)$*-matrix of order* n *that has all the row and column sums equal to* k*, and cylindrical diagonal sums equal to* $\bar{D}=(\bar{d}_1,\bar{d}_2,\ldots,\bar{d}_n)$ *if and only if* $\bar{D}$ *satisfies conditions* (3.11), (3.2) *and* (3.3).

The instance $\bar{D}=(2,4,1,4,5,2)$ of the previous example satisfies conditions (3.11), (3.2) and (3.3). There is at least one $(0,1,2,3)$-matrix that has all the row and column sums equal to 3 and cylindrical diagonal sums $\bar{D}$ (see Fig. 4). This family of $(0,1,2,3)$-matrices contains the following $(0,1)$-matrix that has all the row and column sums equal to 3, and cylindrical diagonal sums equal to $\bar{D}$.



Acknowledgements

The author wishes to thank Volker Strehl whose suggestions greatly improved the presentation of the proof of Theorem 3.3 and for pointing out the existence of Theorem 3.4.

A un amico. Volevo ringraziare Maurice Nivat a cui sono profondamente debitore. I numerosi suggerimenti, le sue intuizioni ed il suo senso estetico sono stati, e tuttora sono per me una guida insostituibile nell'affascinante mondo dei modelli discreti.

References

[1] R.P. Anstee, Invariant sets of arcs in network flow problems, Discrete Appl. Math. 13 (1986) 1–7.
[2] R.A. Brualdi, H. Ryser, Combinatorial Matrix Theory, Cambridge Univ. Press, Cambridge, 1991.
[3] S. Brunetti, A. Del Lungo, P. Gritzmann, S. de Vries, On the reconstruction of permutation and partition matrices under tomographic constraints, preprint.

[4] Y. Caro, Remarks on a Zero-Sum Theorem, J. Combin. Theory, Ser. A 76 (1996) 315–322.
[5] Y. Caro, Zero-sum problems—a survey, Discrete Math. 152 (1996) 93–113.
[6] W.D. Gao, A combinatorial problem on finite abelians groups, J. Number Theory 58 (1996) 100–103.
[7] M. Hall Jr., A combinatorial problem on abelian groups, Proc. Amer. Math. Soc. 3 (1952) 584–587.
[8] Y.O. Hamidoune, On weighted sums in abelian groups, Discrete Math. 162 (1996) 127–132.
[9] G.T. Herman, A. Kuba (Eds.), Discrete Tomography: Foundations, Algorithms and Applications, Birkhauser, Boston, Cambridge, MA, 1999.
[10] R.W. Irving, M.R. Jerrum, Three-dimensional statistical data security problems, SIAM J. Comput. 23 (1994) 170–184.
[11] C. Kisielowski, P. Schwander, F.H. Baumann, M. Seibt, Y. Kim, A. Ourmazd, An approach to quantitative high-resolution transmission electron microscopy of crystalline materials, Ultramicroscopy 58 (1995) 131–155.
[12] G.P.M. Prause, D.G.W. Onnasch, Binary reconstruction of the heart chambers from biplane angiographic image sequence, IEEE Trans. Med. Imaging 15 (1996) 532–559.
[13] F. Salzborn, G. Szekeres, A problem in combinatorial group theory, Ars Combin. 7 (1979) 3–5.
[14] W.A. Schmid, On zero-sum subsequences in finite abelian groups, Integers: Electron. J. Combin. Number Theory 1 (2001) #A01.
[15] A.R. Shliferstein, Y.T. Chien, Switching components and the ambiguity problem in the reconstruction of pictures from their projections, Pattern Recognition 10 (1978) 327–340.